(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－173300
（P2003－173300A）
(43)公開日　平成15年６月20日(2003.6.20)

| (51)Int.Cl.⁷ | | 識別記号 | FI | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06F | 13/00 | 351 | G06F | 13/00 | 351Z　5B085 |
| | 15/00 | 330 | | 15/00 | 330A　5B089 |
| H04L | 12/66 | | H04L | 12/66 | B　5K030 |

審査請求　未請求　請求項の数15　ＯＬ　（全 16 頁）

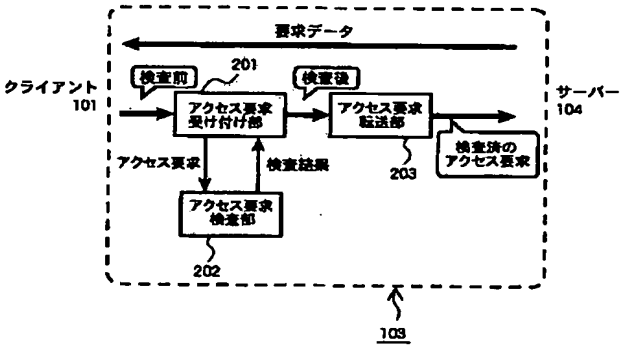
(21)出願番号　特願2002－93667(P2002－93667)
(22)出願日　平成14年３月29日(2002.3.29)
(31)優先権主張番号　特願2001－295368(P2001－295368)
(32)優先日　平成13年９月27日(2001.9.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　菅野　伸一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　楯岡　正道
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　サーバー計算機保護装置、サーバー計算機保護方法、サーバー計算機保護プログラム及びサーバー計算機

(57)【要約】
【課題】　DoSの攻撃からサーバー計算機を保護するサーバー計算機保護装置を提供する。
【解決手段】　クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段（２０２）と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えるサーバー計算機保護装置。



1

【特許請求の範囲】

【請求項１】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、

受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段と、

前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項２】前記アクセス要求検査手段は、前記クライアント計算機が送ってくるアクセス要求パケットが一連の接続要求パケット、確認応答パケット及びデータ要求パケットである場合は、正当なアクセス要求であると判断することを特徴とする請求項１記載のサーバー計算機保護装置。

【請求項３】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、

前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段と、

前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、

前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段と、

前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項４】所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、

前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、

前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段と、

前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項５】パケットのヘッダーを修正するヘッダー修正手段をさらに備え、

前記ヘッダー修正手段は、前記アクセス要求パケットを

2

前記サーバー計算機へ転送する際に前記アクセス要求パケットのヘッダーを修正することを特徴とする請求項１乃至４記載のサーバー計算機保護装置。

【請求項６】　前記サーバー計算機から前記クライアント計算機への応答を代わりに行う代理応答部をさらに備え、

前記代理応答部は前記クライアント計算機と前記サーバー計算機保護装置との間でコネクションを確立した後に、代理応答を行うことを特徴とする請求項１乃至４記載のサーバー計算機保護装置。

【請求項７】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、

正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項８】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、

前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項９】所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項１０】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、
正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項１１】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、
前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、
前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、
前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、
前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項１２】所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、
前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、
前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、
前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項１３】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、
前記サーバー計算機はサーバー計算機保護装置を含み、
前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【請求項１４】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、
前記サーバー計算機はサーバー計算機保護装置を含み、



前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段と、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【請求項１５】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、
前記サーバー計算機はサーバー計算機保護装置を含み、
前記サーバー計算機保護装置は、所定のクライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアント計算機とサーバー計算機間のネットワークシステムに関し、特に、意図的にサーバー計算機の処理を妨害する不正なアクセスからサーバー計算機を保護するサーバー計算機保護装置に関する。

【０００２】

【従来の技術】近年、インターネット等を利用し、不特定多数あるいは特定多数のクライアント計算機をパケット交換ネットワーク経由でサーバー計算機に接続し、クライアント計算機からの要求に応じてサーバー計算機からデータを供給することを目的とする計算機サーバーシステムが広く使われている。ここで、パケットとは、ネットワーク上を流れるひとかたまりのデータをいい、大まかに分けると、ヘッダーとデータ本体で構成されている。さらに、ヘッダー内には、送信先のＩＰ(Internet Protocol)アドレス、宛先のＩＰアドレス、パケットの

前後関係を表す伝送シーケンス番号等から構成されている。

【０００３】しかしながらこのようなシステムの妨害を意図した不正なアクセスによる攻撃が増加する傾向にある。

【０００４】特に、一つのクライアント計算機から同時に大量に同じようなアクセス要求をサーバー計算機に対して行うことによって、標的となるサーバー計算機のデータ供給サービスを不能にする攻撃方法(以下、DoS攻撃(Denial of Service attack)と表記)は、正当なクライアントからのアクセスとの区別がつきにくく有効な対策をとることが困難である。尚、このDoS攻撃を複数のクライアント計算機が行う場合をDDoS攻撃(Distributed Denial of Service attack)という。

【０００５】ここで、クライアント計算機からサーバー計算機への正当なアクセス要求とは、実際にサーバー計算機からデータを受け取ったアクセス要求をいう。TCP/IP(Transmission Control Protocol/IP) プロトコルにおける正当なアクセス要求の一例としては、 クライアント計算機はサーバー計算機へ接続要求パケット（SYN(SYNchronousness)パケット）を送り、 サーバー計算機はクライアント計算機へ接続要求確認パケット（SYN+ACK(ACKnowledgement)パケット）を送り、 クライアント計算機はサーバー計算機へ確認応答パケット（ACKパケット）を送ることによって、論理的な通信路（コネクション）が確立する（３ウェイ・ハンドシェーク方式）。 このコネクション確立（Established）状態で、クライアント計算機はサーバー計算機へデータ要求パケット（URL(Uniform Resource Locator)パケット）を送り、 サーバー計算機はクライアント計算機へURLパケットによって要求されたデータパケットを送り、実際にクライアント計算機が受け取るという手順がある。

【０００６】インターネットにおけるこのようなDoS攻撃の一般的な方法としては、以下のような妨害方法が挙げられる。

【０００７】（１）SYNパケットのみをサーバー計算機の処理能力を超えるぐらい大量に送りつけ、サーバー計算機がSYN+ACKパケットを送れないようにする方法（以下 SYN flood と表記）

（２）SYNパケット及びACKパケットを大量にサーバー計算機へ送り、このサーバー計算機との間でコネクションを確立したが、その後URLパケットを一定時間以内に送らず放置する方法（以下 Established flood と表記）

（３）通常のクライアントと同様にコネクション確立状態でURLパケットを送る正当なアクセスだが、この正当なアクセスを大量に行うことによって、意図的にサーバー計算機の処理を妨害する方法（例えば、予め決めた時間に、たくさんの人が特定のサーバー計算機にアクセスする場合；DDoS攻撃）（以下、Accessflood と表記）

このような攻撃をサーバー計算機が受けると、接続要求毎にデータ供給用メモリを確保するためにサーバー計算機内の記憶装置等の資源を浪費してしまい、妨害を意図していないクライアント計算機からの通常のアクセスが大きく滞ることになる。

【０００８】そこで、これらの攻撃からサーバー計算機を保護する目的で、サーバーとネットワークの間に配置するサーバー計算機保護装置においては、SYN flood に対しては、複数回の接続要求が繰り返されたもののみを正当な接続要求として処理したり、既に正当なアクセスがあったクライアントからのアクセスを正当な接続要求として処理し、それ以外のアクセスについてはパケットを破棄する方法などが従来取られている。

【０００９】しかし、このような方法では攻撃側が複数回の同じ接続要求を出したりする方法を取ることにより攻撃が成立するという問題点があり、また Established flood や Access flood については対抗することができないという問題がある。

【００１０】

【発明が解決しようとする課題】DoS攻撃に対し、これらの攻撃の影響からサーバー計算機を保護し、正当なしかも妨害を意図していないクライアントからのサービスを大きく滞らせることなく行うことを課題とする。

【００１１】

【課題を解決するための手段】第１の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段（２０２）と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えるサーバー計算機保護装置である。

【００１２】第２の発明は、前記アクセス要求検査手段は、前記クライアント計算機が送ってくるアクセス要求パケットが一連の接続要求パケット、確認応答パケット及びデータ要求パケットである場合は、正当なアクセス要求であると判断することを特徴とする第１の発明記載のサーバー計算機保護装置である。

【００１３】第３の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段（３０３）と、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（３０１）と、前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバ

一計算機の負荷状態を検査するサーバー負荷検査手段（３０２）と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えるサーバー計算機保護装置である。

【００１４】第４の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（３０１）と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段（３０２）と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えるサーバー計算機保護装置である。

【００１５】第５の発明は、パケットのヘッダーを修正するヘッダー修正手段（２１０）をさらに備え、前記ヘッダー修正手段は、前記アクセス要求パケットを前記サーバー計算機へ転送する際に前記アクセス要求パケットのヘッダーを修正することを特徴とする第１乃至第４の発明記載のサーバー計算機保護装置である。

【００１６】第６の発明は、前記サーバー計算機から前記クライアント計算機への応答を代わりに行う代理応答部（５０１）をさらに備え、前記代理応答部は前記クライアント計算機と前記サーバー計算機保護装置との間でコネクションを確立した後に、代理応答を行うことを特徴とする第１乃至第４の発明記載のサーバー計算機保護装置である。

【００１７】第７の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【００１８】第８の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【００１９】第９の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【００２０】第１０の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【００２１】第１１の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【００２２】第１２の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【００２３】第１３の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であっ

て、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段（２０２）と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えることを特徴とするサーバー計算機である。

【００２４】第１４の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段（３０３）と、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（３０１）と、前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段（３０２）と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えることを特徴とするサーバー計算機である。

【００２５】第１５の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、所定のクライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（２０１）と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（３０１）と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段（３０２）と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（２０３）と、を備えることを特徴とするサーバー計算機である。

【００２６】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【００２７】図１は、本発明の実施形態に係るサーバー計算機保護装置が適用されるネットワークシステムの概要図である。サーバー計算機１０４は、サーバー計算機保護装置１０３を介してネットワーク１０２に接続されており、また、このネットワーク１０２に接続されているクライアント計算機１０１とのデータパケットのやり取りには必ずサーバー計算機保護装置が仲介している。

【００２８】（第１の実施の形態）図２は、第1の実施形態に係るサーバー計算機保護装置１０３のブロック図である。保護装置１０３は、アクセス要求受け付け部２０１と、アクセス要求検査部２０２と、アクセス要求転送部２０３を含んでいる。

【００２９】クライアント計算機１０１からのアクセス要求つまり検査前のアクセス要求はアクセス要求受け付け部２０１で受け取り、その後アクセス要求検査部２０２に転送される。アクセス要求のパケットには、接続要求パケット（SYNパケット）、確認応答パケット（ACKパケット）及びデータ要求パケット（URLパケット）の３段階のパケットがある。

【００３０】検査結果はアクセス要求受け付け部２０１に入り、検査後のアクセス要求がアクセス要求転送部２０３に送られる。そして、検査済のアクセス要求がアクセス要求転送部２０３からサーバー計算機１０４へ出力される。

【００３１】以下、保護装置１０３全体の処理の流れを図3のフローチャートを用いて説明する。保護装置１０３は、クライアント計算機１０１から接続要求パケット（SYNパケット）を受け取ると、クライアント計算機へSYN+ACKパケットを送り（Ｓ１０１）、次の段階のアクセス要求（ACKパケットまたはURLパケット）待ち状態になる（Ｓ１０２）。

【００３２】そして、不正アクセスか否かを判断する（Ｓ１０３）。判断の一例としては、クライアント計算機１０１からのアクセス要求は、保護装置１０３内のアクセス要求受け付け部２０１により受領し、アクセス要求検査部２０２でアクセス要求の内容を検査する。　本実施形態で検査できる不当なアクセス要求は、従来の技術で説明したSYN floodとEstablished floodの２種類である。そして、正当なアクセス要求とはコネクション確立状態で一定時間以内にURLパケットを送ってくる場合をいう。

【００３３】検査の結果、正当なアクセス要求だと認められた場合、アクセス要求転送部２０３はサーバーと接続し（Ｓ１０４）、正当なアクセス要求をサーバー計算機１０４に転送する（Ｓ１０５）。そして、サーバー計算機１０４はURLパケットによって指定されたデータをパケット単位で保護装置１０３を介してクライアント計算機１０１に供給する（Ｓ１０６）。保護装置１０３は

データの供給が完了してからサーバー計算機１０４との接続を切断し（Ｓ１０７）、クライアント計算機１０１との接続も切断する。一方、不当なアクセス要求であると判断した場合は、Ｓ１０３からすぐにＳ１０８のクライアントとの切断処理が実行される。

【００３４】したがって、従来の技術で説明したSYN flood,Established flood等のDoS撃からサーバー計算機を保護できる。

【００３５】尚、アクセス要求検査部２０２の正当なアクセス要求であるか否かの判断基準としては、上述したようなSYNパケットのみを送りつけてくるようなアクセス要求が所定の伝達形式から外れていないかどうかの他に、サーバー計算機１０４にはありえないアクセス（例えば、不当なURLパケット）を要求しているかどうか等がある。

【００３６】本実施形態の変形例としては、検査前の全段階のアクセス要求はアクセス要求受け付け部２０１に入ると同時に、アクセス要求転送部２０３にも送られ、データ要求検査部２０２の検査結果をデータ要求転送部２０３が受け取ってから、サーバ計算機１０４へアクセス要求を出力しても良い。

【００３７】（第２の実施の形態）図４は第２の実施形態に係るサーバー計算機保護装置１０３のブロック図である。本実施形態の特徴は、第１の実施形態で説明したアクセス要求の内容を検査するアクセス要求検査部の代わりに、クライアント計算機１０１から送られてくる接続要求パケット（SYNパケット）の数が所定の値を超えた場合、すなわち、サーバー計算機１０４の負荷が過大になった場合には、サーバー計算機１０４へアクセス要求を転送するのを止めることである。

【００３８】クライアント計算機１０１からのあるSYNパケットをデータ要求受け付け部２０１及び接続要求数計測部３０３により受け取る。データ供給数計測部３０１は、常にサーバー計算機１０４が所定時間に供給するデータ供給数を計測する。ここで、接続要求数とはある接続要求を受け付けたときに全てのクライアント計算機から届いたSYNパケットの総数をいい、通常、一つのクライアント計算機とサーバー計算機との間には複数のコネクションが張られる。また、データ供給数とは、成立しているコネクションのうち、ある接続要求を受け付けたときに実際にデータ供給している数をいう。

【００３９】以下、保護装置１０３全体の処理の流れを図５（ａ）のフローチャートを用いて説明する。保護装置１０３は接続要求待ち（Ｓ２０１）の状態から、接続要求数計測部３０３でクライアント計算機１０１からのSYNパケットを検知すると、サーバー負荷検査部３０２はデータ供給数計測部３０１及び接続要求数計測部３０３の出力結果を用いて、サーバー計算機１０４の負荷が過大か否かを検査する（Ｓ２０２）。判断基準の一例としては、データ要求数（URLパケットの総数）に比べてデータ供給数が少ない場合に負荷が過大であるが挙げられる。

【００４０】所定の負荷を超えていない場合には、クライアント計算機と接続し（Ｓ２０３）、データ要求待ち（Ｓ２０４）状態となる。この時、サーバー負荷検査部３０２は接続数を１増加させる（Ｓ２０５）。

【００４１】続いて、サーバーと接続し（Ｓ２０６）、クライアント計算機１０３からのデータ要求パケットをサーバーに転送する（Ｓ２０７）。そして、サーバー計算機１０４がクライアント計算機にデータを供給してから（Ｓ２０８）、保護装置１０３はクライアント計算機１０１及びサーバー計算機１０４との接続を切断し（Ｓ２０９）、サーバー負荷検査部３０２は接続数を１減少させる（Ｓ２１０）。

【００４２】一方、所定の負荷を超えていた場合には接続要求待ちの状態（Ｓ２０１）に戻る。これにより、DoS攻撃によってサーバーの負荷が過大になるのを防止し、サーバーの処理速度低下を防止することができる。

【００４３】図５（ｂ）は、同図（ａ）のＳ２０２で所定の負荷を超えていた場合の変形例である。すなわち、Ｓ２０２で所定の負荷を超えていた場合（所定の接続数を超えていた場合）であって、保護装置１０３が処理できる接続数を超える場合には、接続処理が完了していないコネクションのうち最も古いものを破棄してから（Ｓ２０２’のｙ）、クライアント計算機と接続する（Ｓ２０３）。以降の処理は、同図（ａ）と同じである。一方、Ｓ２０２で所定の負荷を超えている場合であるが、保護装置１０３が処理できる接続数を超えていない場合には、接続要求待ちの状態（Ｓ２０１）に戻る。　このように、コネクションのうち最も古いものを破棄することによって、保護装置自体へDoS攻撃を受けた時でもサービスを続行できる。

【００４４】（第３の実施の形態）図６は、第３の実施形態に係るサーバー計算機保護装置１０３のブロック図である。図７は本実施形態に係るフローチャートである。本実施形態はアクセス要求を送ってきたクライアント計算機毎にデータ供給数計測部３０１及びサーバー負荷検査部３０２を設けることを特徴とする。

【００４５】まず、保護装置１０３は、接続要求待ちの状態（Ｓ３０１）から、特定のクライアント計算機からSYNパケット及びACKパケットを受けると、前記特定のクライアント計算機との間でコネクションを張り（Ｓ３０２）、前記特定のクライアント計算機専用のデータ供給数計測部３０１及びサーバー負荷計算部３０２（以下、本実施形態に限ってデータ供給数計測部３０１及びサーバー負荷計算部３０２と省略する）を設ける。尚、データ供給数計測部３０１及びサーバー負荷計算部３０２は、単純な計算機能を有していれば良いので、保護装置１０３のメモリ及びＣＰＵの消費は少ない。したがって、クライアント計算機毎に１０００～１００００個ぐ

らい設けることができる。

【００４６】次に、前記特定のクライアント計算機からのアクセス要求待ちの状態になり（Ｓ３０４）、前記特定のクライアント計算機からアクセス要求が来ると、アクセス要求受け付け部２０１からすぐにアクセス要求伝達部２０３へ行き、サーバー計算機１０４とコネクションを張る（Ｓ３０５）。

【００４７】データ供給数計測部３０１は、現在サーバー計算機１０４が伝送中の要求されたデータを送付した特定のクライアント計算機へのデータ供給状況を計測することによって、特定のクライアント計算機に対するサーバーの負荷が過大か否かを判断する（Ｓ３０６）。所定の負荷を超えていない場合には、サーバー負荷検査部３０２は、アクセス要求転送部２０３へサーバー計算機１０４にURLパケットを転送するように指示をし（Ｓ３０７）、サーバー計算機１０４が要求されたデータを特定のクライアント計算機に供給し（Ｓ３０８）、データ供給が完了したら特定のクライアント計算機及びサーバー計算機との接続を切断する。

【００４８】一方、所定の負荷を超えていた場合には、データ要求転送部２０３がデータ要求パケットをサーバー計算機１０４に転送するのを保留するために再度Ｓ３０６の処理を行い、特定のクライアント計算機へのデータ供給数が減少するのを待つ。

【００４９】これにより、サーバー計算機１０４の負荷が過大になるのを防止するとともに、特定のクライアント計算機によるサーバー計算機１０４の独占状態を回避し、他のクライアント計算機へのデータ供給を阻害されることを減少できる。したがって、従来の技術で説明したAccess floodに対応することもできる。

【００５０】（第４の実施の形態）図８は、第4の実施形態に係るサーバー計算機保護装置１０３のブロック図であり、本実施形態は、第１の実施形態と基本的に同じであるが、ヘッダー修正部２１０を備えていることを特徴とする。

【００５１】例えばTCP/IPでは、接続処理にあたりヘッダー内に、伝送シーケンス番号を付与しパケットの前後関係を制御している。接続開始にあたってこれらは送受双方向にてサーバー計算機とクライアント計算機のやりとりで決定される。

【００５２】しかし、本実施形態を利用する場合にはサーバー計算機１０４への接続動作（図３のＳ１０４）はデータ要求の正当性の検査後になる（図３のＳ１０３）ので、保護装置１０３が任意に発生した保護装置用シーケンス番号でクライアント計算機１０１と接続処理を行わざるをえない（図３のＳ１０１）。この保護装置用シーケンス番号は検査後に行われるサーバー計算機との接続処理（図３のＳ１０４）においてサーバー計算機１０４から通知されるサーバー計算機用シーケンス番号と異なるため、そのまま要求されたデータのパケットを伝送すると TCP/IPプロトコルを使用したデータ伝送が不可能である。そこで、ヘッダー修正部２１０を用いこれらのシーケンス番号の差分を修正し、また他のヘッダー情報（例えば送信先のＩＰアドレス、宛先のＩＰアドレス）を必要があれば整合が取れるように修正することによりサーバー計算機１０４からクライアント計算機１０１への通信を成立させることができる。

【００５３】一例としては、一つのデータ要求に対して以下の　～　の処理を行っている。

【００５４】　クライアント計算機１０１からの接続要求をデータ要求受け付け部２０１、データ要求検査部２０２及びデータ転送伝達部２０３によって検査後に、クライアント計算機１０１とサーバー計算機１０４とのコネクションを確立する。

【００５５】　このコネクションを経由して送られてくるクライアント計算機１０１からのデータ要求パケットのヘッダーをヘッダー修正部２１０で修正してから、サーバー計算機１０４へ転送する。

【００５６】　このコネクションを経由して送られてくるサーバー計算機１０４からのデータパケットのヘッダーをヘッダー修正部２１０で修正してから、クライアント計算機１０１へ転送する。

【００５７】（第５の実施形態）図９は、第５の実施形態に係るサーバー計算機保護装置１０３のブロック図である。本実施形態は、第２の実施形態と基本的に同じであるが、第４の実施形態で説明したヘッダー修正部２１０を備えていることを特徴とする。

【００５８】尚、ヘッダー修正部２１０がハッシュ関数を用いてクライアント計算機１０１とサーバー計算機１０４とのコネクションを管理する方法を利用した場合には、図５のＳ２０２の代わりに、該ハッシュのテーブルが溢れたことをもってサーバー計算機１０４の負荷を過大であると判断しても良い。

【００５９】（第６の実施形態）図１０は、第６の実施形態に係るサーバー計算機保護装置１０３のブロック図である。本実施形態は、第３の実施形態と基本的に同じであるが、第４の実施形態で説明したヘッダー修正部２１０を備えていることを特徴とする。

【００６０】（他の実施形態）本発明は上記実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲内で適宜変更できる。以下、変形例について説明する。

【００６１】（変形例１）図１１は、変形例１に係るサーバー計算機保護装置１０３のブロック図である。本変形例は、第６の実施形態の変形例であり、保護装置１０３とサーバー計算機１０４との接続数を計測するサーバー接続数計測部４０１を備えていることを特徴とする。このサーバー接続数計測部４０１の出力結果はクライアント計算機毎に設けられたサーバー負荷検査部３０２に入力されている。また、クライアント計算機毎の接続数

は、クライアント計算機毎に設けられたデータ供給数３０１で計測できる。したがって、いずれの接続数も保護装置１０３内部で計測できるので、クライアント計算機毎のサーバー負荷検査処理も簡易化できる。

【００６２】（変形例２）変形例２は、第４の実施形態の変形例であり、保護装置１０３には、クライアント計算機との間でコネクション成立後、データ要求パケットが届くまでの時間を計測する時計部を有している。そして、この時計部を用いて、データ要求受け付け部２０１が予め規定した時間の間に所定の形式のデータ要求が届かない場合には不正なアクセスと判断し、コネクションを破棄する。これによりサーバー計算機保護装置内部の資源が過大になることを防ぎ、なおかつ正当なクライアントからの接続動作に早い段階でメモリーなどの資源を振り向けることができるようになる。

【００６３】また、上述した時計部を用いて、データ要求受け付け部２０１はコネクションを確立してから最も経過時間が長いものを不正なアクセスと判断して、コネクションを破棄しても良い。

【００６４】さらに、データ要求受け付け部２０１は、上述した時計部を用いて一定時間内に同一クライアントからの同一データに対する要求回数を計測する機能を有すれば、この計測し、あらかじめ設定した一定時間内の同一データ要求回数の限度を超えた場合に不正なアクセスとして判断して、コネクションを破棄しても良い。

【００６５】（変形例３）図１２及び図１３は、変形例３に係るサーバー計算機保護装置１０３のブロック図及びフロチャートである。本変形例は、他の実施形態に適用可能であり、サーバー計算機１０４の代りにクライアント計算機１０１へ応答する代理応答部５０１を備えていることを特徴とする。代理応答部５０１がサーバー計算機１０４に成り代わるためには、図８で説明したヘッダー修正部２１０を備えていればよい。

【００６６】クライアント計算機１０１と保護装置１０３とがTCP/IPプロトコルでコネクションを確立する手順は上述した通りである（Ｓ４０１～Ｓ４０４）。その後（、すなわち、クライアント計算機１０１からのデータ要求が来る前）に、代理応答部５０１は、サーバー計算機１０４からクライアント計算機１０１への応答を代わりに行う（Ｓ４０５）。

【００６７】ここでの応答とは、TCP/IPの上位プロトコル、例えば、SMTP(Simple Mail Transfer Protocol)の場合は、サーバー計算機１０４がメールを受け取ることが可能であるという状態を示す応答であり、また、POP(Post Office Protocol)の場合には、POPのバージョン（例えば、POP3）を応答する。そして、応答の具体例としては、サーバー計算機１０４が正常動作している場合にクライアントに返答する内容と同等のもの、あるいは、保護装置１０３とサーバー計算機１０４との間で直前に行われた上位プロトコルによる接続動作によりサーバー計算機１０４が返答したものと同様の内容のもの等が挙げられる。

【００６８】この応答を受けることによって、クライアント計算機１０１は、サーバー計算機１０４と上位プロトコルで接続動作が行われたと判断し、データ転送要求等の次の動作に移行する。

【００６９】クライアント計算機１０１からのデータ要求は、要求受付部２０１で受け付け、要求検査部２０２でデータ要求の内容を検査した後に、サーバー計算機１０４に伝達する。サーバー計算機１０４は、伝達された内容に基づき所定のデータをクライアント計算機１０１に返送する。その後、上述した切断手順を行う（Ｓ４０６～Ｓ４１７）。ここでの検査としては、データ要求が所定の伝達形式から外れていないかどうか、ありえないデータを要求しているかどうか等が挙げられる。

【００７０】尚、上述したように、クライアント計算機１０１からのデータ要求が正常であった場合には、保護装置１０３はサーバー計算機１０４に接続動作を行い、クライアント計算機１０１の要求をサーバー計算機１０４に伝達する。この接続後にサーバー計算機１０４が応答するものには、先に保護装置１０３がサーバー計算機１０４に応答したものと重複する場合がある。それゆえ、データ要求の処理に齟齬を来さない場合にはこの応答をクライアントに伝達しない。もし、齟齬を来す場合には保護装置１０３はサーバー計算機１０４とクライアント計算機１０１との接続を破棄する処理を行う。

【００７１】他の変形例としては、上述したサーバー計算機保護装置はサーバー計算機の中に含まれていても良い。この場合、サーバー計算機保護装置専用のメモリ等のハードウェアがサーバー計算機内にあれば良い。

【００７２】（記録媒体への適用）また、本実施形態における処理をコンピュータで実行可能なプログラムで実現し、このプログラムをコンピュータで読み取り可能な記憶媒体として実現することも可能である。

【００７３】なお、本記憶媒体としては、磁気ディスク、フレキシブルディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ，ＣＤ－Ｒ，ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【００７４】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼動しているＯＳ（オペレーションシステム）や、データベース管理ソフト、ネットワーク等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【００７５】さらに、本記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【００７６】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も、本発明における記憶媒体に含まれ、媒体の構成は何れの構成であってもよい。

【００７７】なお、上記コンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【００７８】また、上記コンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本実施形態の機能を実現することが可能な機器、装置を総称している。

【００７９】

【発明の効果】上述したように本発明によれば、DoS攻撃に対し、これらの攻撃の影響からサーバー計算機を保護し、正当なしかも妨害を意図していないクライアントからのサービスを大きく滞らせることなく行うことができる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るサーバー計算機保護装置が適用されるネットワークシステムの概要図。

【図２】　本発明の第１の実施形態に係るサーバー保護装置のブロック図。

【図３】　第１の実施形態に係るフローチャート。

【図４】　本発明の第２の実施形態に係るサーバー保護装置のブロック図。

【図５】　第２の実施形態に係るフローチャート。



【図６】　本発明の第３の実施形態に係るサーバー保護装置のブロック図。

【図７】　第３の実施形態に係るフローチャート。

【図８】　本発明の第４の実施形態に係るサーバー保護装置のブロック図。

【図９】　本発明の第５の実施形態に係るサーバー保護装置のブロック図。

【図１０】　本発明の第６の実施形態に係るサーバー保護装置のブロック図。

【図１１】　本発明の変形例１に係るサーバー保護装置のブロック図。

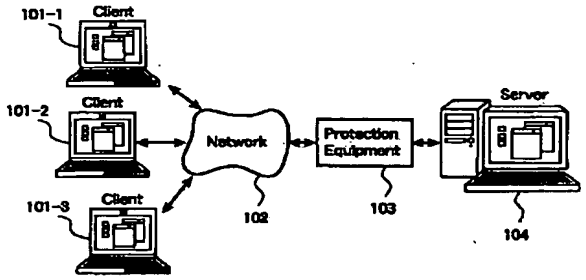
【図１２】　本発明の変形例３に係るサーバー保護装置のブロック図。

【図１３】　本発明の変形例３に係るに係るフローチャート。

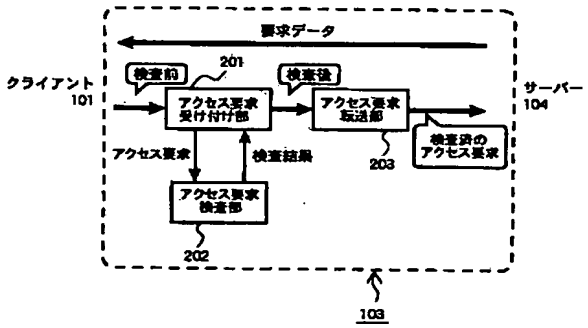
【符号の説明】

１０１　クライアント計算機
１０２　ネットワーク
１０３　サーバー計算機保護装置
１０４　サーバー計算機
２０１　データ要求受け付け部
２０２　データ要求検査部
２０３　データ要求転送部
３０１　データ供給数計測部
３０２　サーバー負荷検査部
３０３　接続要求数計測部
４０１　サーバー接続数計測部
５０１　代理応答部

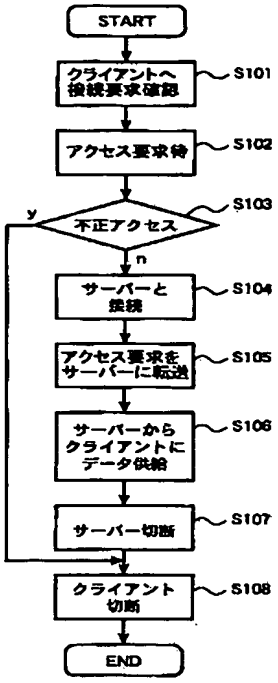
【図１】



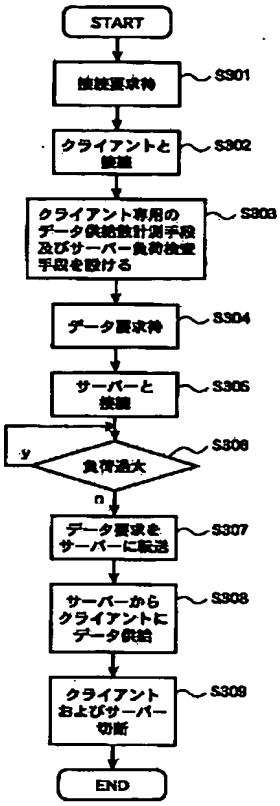

【図２】



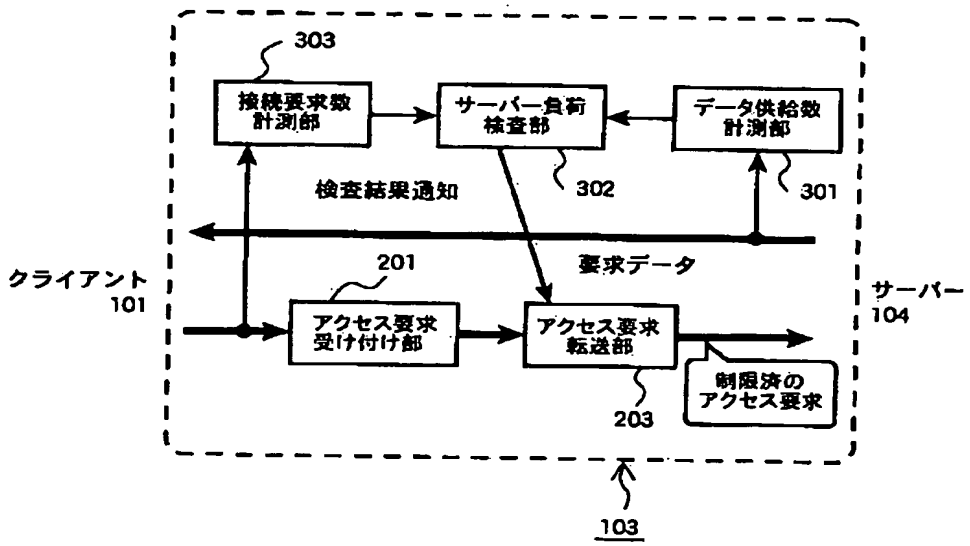
【図３】


START
クライアントへ接続要求確認
S101
アクセス要求待
S102
不正アクセス
S103
y
n
サーバーと接続
S104
アクセス要求をサーバーに転送
S105
サーバーからクライアントにデータ供給
S106
サーバー切断
S107
クライアント切断
S108
END

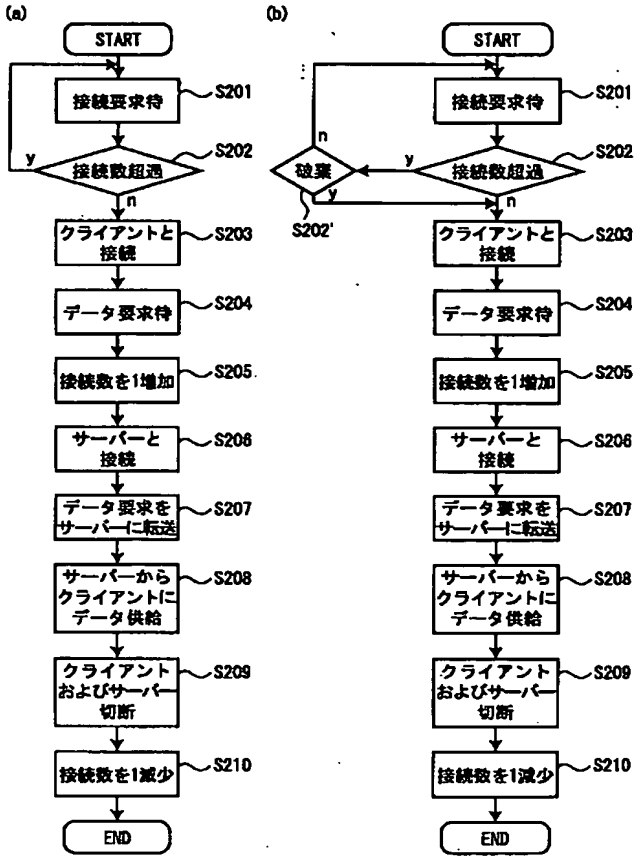
【図７】


START
接続要求待
S301
クライアントと接続
S302
クライアント専用のデータ供給数計測手段及びサーバー負荷検査手段を設ける
S303
データ要求待
S304
サーバーと接続
S305
y
負荷過大
S306
n
データ要求をサーバーに転送
S307
サーバーからクライアントにデータ供給
S308
クライアントおよびサーバー切断
S309
END

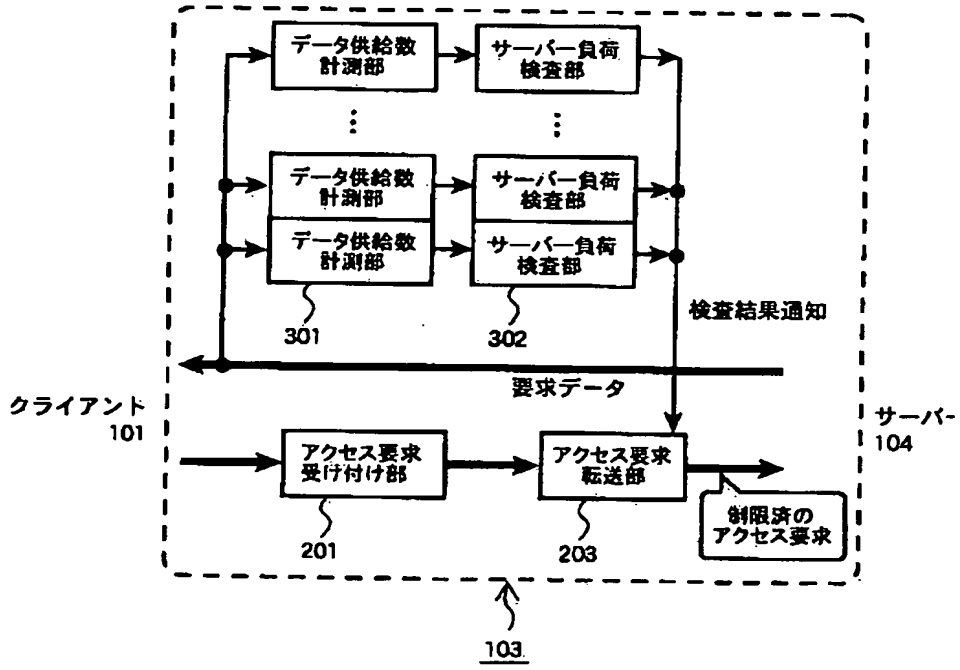
【図４】


303
接続要求数計測部
サーバー負荷検査部
データ供給数計測部
検査結果通知
302
301
クライアント
101
201
要求データ
サーバー
104
アクセス要求受け付け部
アクセス要求転送部
制限済のアクセス要求
203
103

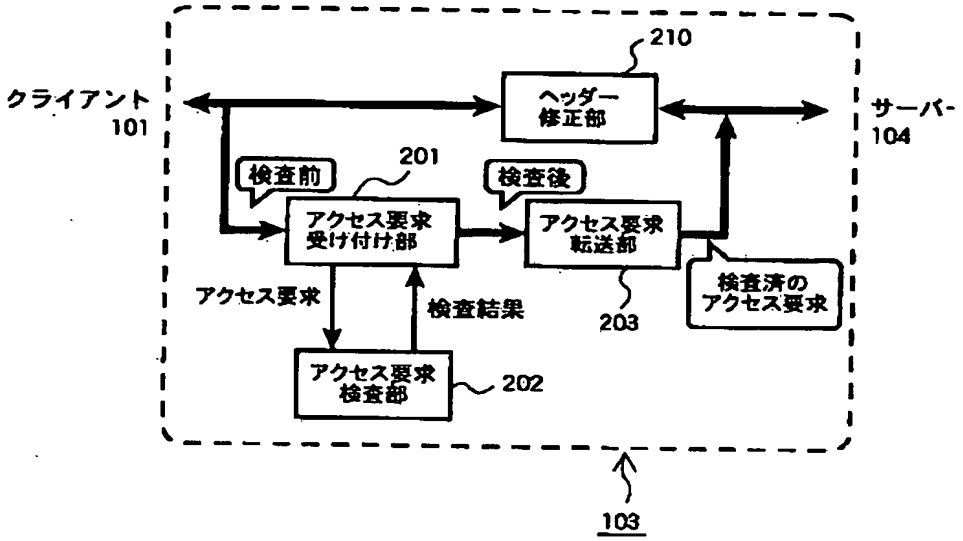
【図５】


(a)
START
接続要求待
S201
接続数超過
S202
y
n
クライアントと接続
S203
データ要求待
S204
接続数を1増加
S205
サーバーと接続
S206
データ要求をサーバーに転送
S207
サーバーからクライアントにデータ供給
S208
クライアントおよびサーバー切断
S209
接続数を1減少
S210
END
(b)
START
接続要求待
S201
破棄
n
y
接続数超過
S202
S202'
クライアントと接続
S203
データ要求待
S204
接続数を1増加
S205
サーバーと接続
S206
データ要求をサーバーに転送
S207
サーバーからクライアントにデータ供給
S208
クライアントおよびサーバー切断
S209
接続数を1減少
S210
END

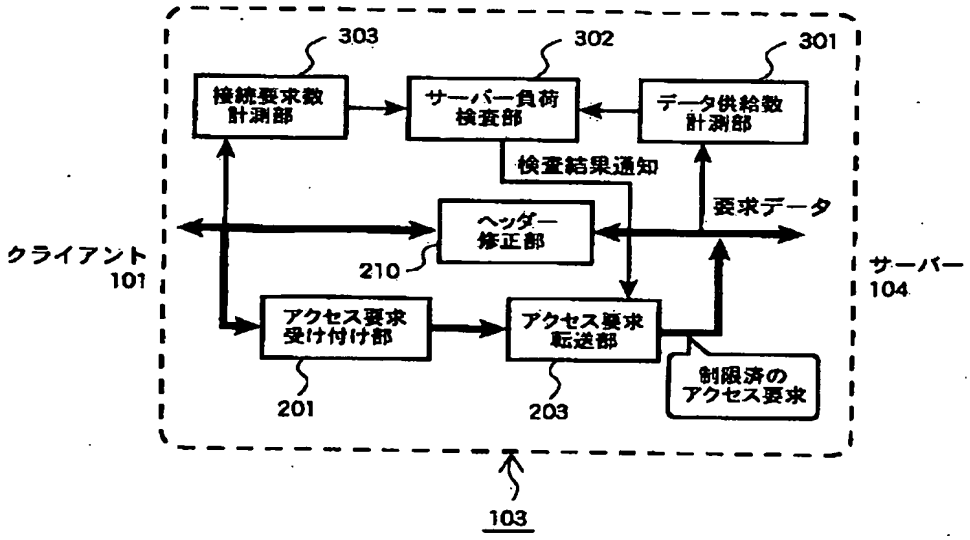
【図６】


データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
301
302
検査結果通知
要求データ
クライアント
101
サーバー
104
アクセス要求受け付け部
アクセス要求転送部
制限済のアクセス要求
201
203
103

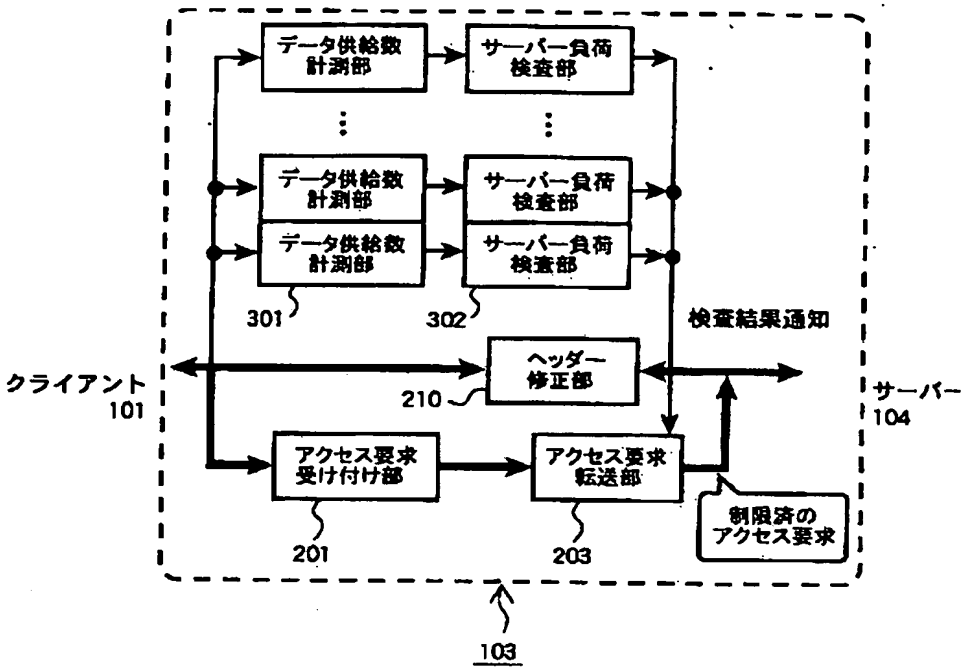
【図８】


クライアント
101
210
ヘッダー
修正部
サーバ-
104
検査前
201
検査後
アクセス要求
受け付け部
アクセス要求
転送部
検査済の
アクセス要求
アクセス要求
検査結果
203
アクセス要求
検査部
202
103

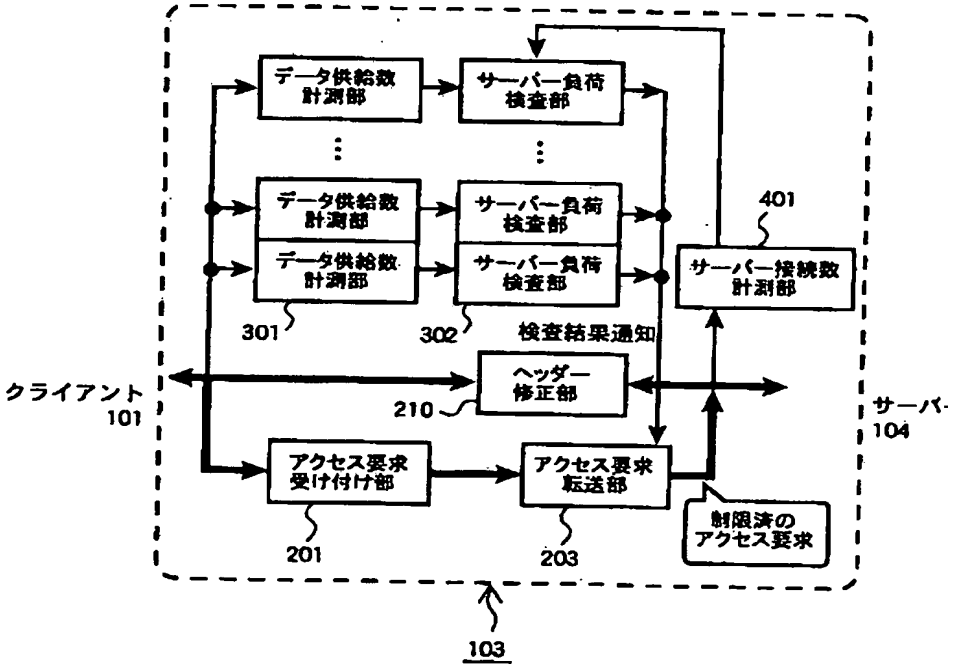
【図９】


303
302
301
接続要求数
計測部
サーバー負荷
検査部
データ供給数
計測部
検査結果通知
要求データ
ヘッダー
修正部
210
クライアント
101
サーバー
104
アクセス要求
受け付け部
アクセス要求
転送部
制限済の
アクセス要求
201
203
103

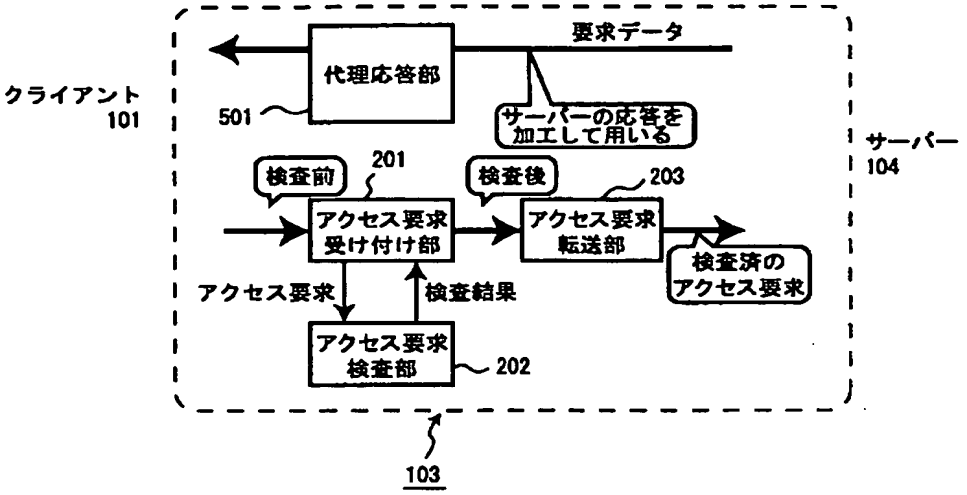
【図１０】


データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
301
302
検査結果通知
ヘッダー修正部
210
クライアント101
サーバー104
アクセス要求受け付け部
アクセス要求転送部
制限済のアクセス要求
201
203
103

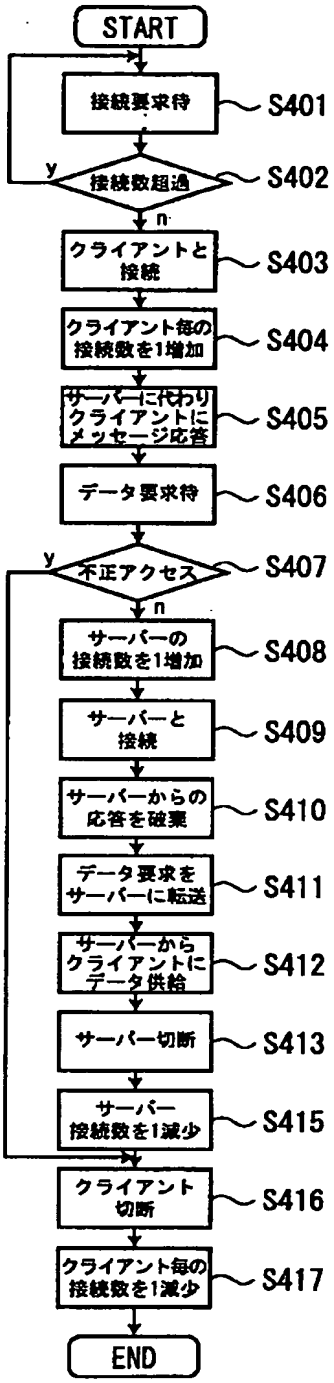
【図１１】


データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
データ供給数計測部
サーバー負荷検査部
401
サーバー接続数計測部
301
302
検査結果通知
ヘッダー修正部
210
クライアント101
サーバー104
アクセス要求受け付け部
アクセス要求転送部
制限済のアクセス要求
201
203
103

【図１２】


クライアント
101
代理応答部
501
要求データ
サーバーの応答を
加工して用いる
サーバー
104
検査前
201
検査後
203
アクセス要求
受け付け部
アクセス要求
転送部
検査済の
アクセス要求
アクセス要求
検査結果
アクセス要求
検査部
202
103

【図１３】




フロントページの続き

Ｆターム(参考) 5B085 AE00 BA06 BG07
5B089 GA11 GA19 GB01 GB02 KA06
KA17 KB13 MA07
5K030 GA15 MB09